TW AF

PTO/SB/21 (04-07)
Approved for use through 09/30/2007. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	10/702,540
Filing Date	November 7, 2003
First Named Inventor	SO, Vincent
Art Unit	3621
Examiner Name	AGWUMEZIE, Charles C.
Attorney Docket Number	79865-5
Total Number of Pages in This Submission	52

ENCLOSURES *(Check all that apply)*

- □ Fee Transmittal Form
  - □ Fee Attached
- □ Amendment / Reply
  - □ After Final
  - □ Affidavits/declaration(s)
- □ Extension of Time Request
- □ Express Abandonment Request
- □ Information Disclosure Statement
- □ Certified Copy of Priority Document(s)
- □ Reply to Missing Parts/ Incomplete Application
  - □ Reply to Missing Parts under 37 CFR 1.52 or 1.53

- □ Drawing(s)
- □ Licensing-related Papers
- □ Petition
- □ Petition to Convert to a Provisional Application
- □ Power of Attorney, Revocation Change of Correspondence Address
- □ Terminal Disclaimer
- □ Request for Refund
- □ CD, Number of CD(s) ________
  - □ Landscape Table on CD

- □ After Allowance Communication to TC
- □ Appeal Communication to Board of Appeals and Interferences
- ☒ Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- □ Proprietary Information
- □ Status Letter
- ☒ Other Enclosure(s) (please identify below):

Return Receipt Postcard.

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	SMART & BIGGAR		
Signature			
Printed name	R. ALLAN BRETT		
Date	September 19, 2007	Reg. No.	40,476

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria,VA 22313-1450 on the date shown below:

Signature			
Typed or printed name		Date	

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

TRANSMITTAL OF APPEAL BRIEF (Small Entity)	Docket No. **79865-5**

In Re Application Of: **SO, Vincent**

Application No.	Filing Date	Examiner	Customer No.	Group Art Unit	Confirmation No.
10/702,540	**November 7, 2003**	**AGWUMEZIE, Charles C.**	**07380**	**3621**	**8250**

Invention: **INTERNET BASED DATA CONTENT RENTAL SYSTEM AND METHOD**

COMMISSIONER FOR PATENTS:

Transmitted herewith is the Appeal Brief in this application, with respect to the Notice of Appeal filed on:

July 27, 2007

☒ Applicant claims small entity status. See 37 CFR 1.27

The fee for filing this Appeal Brief is: **$250.00**

☐ A check in the amount of the fee is enclosed.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. 19-2550. I have enclosed a duplicate copy of this sheet.

☐ Payment by credit card. Form PTO-2038 is attached.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

Signature

Dated: **September 19, 2007**

R. Allan Brett

Reg. No. 40,476

Tel No. 613-232-2486

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)] on

____________________.
(Date)

Signature of Person Mailing Correspondence

Typed or Printed Name of Person Mailing Correspondence

cc:

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No. : 10/702,540 Confirmation No. 8250
Applicant : Vincent So
Filed : November 7, 2003
TC/A.U. : 3621
Examiner : Charles C. Agwumezie

Docket No. : 79865-5
Customer No. : 07380

MAILSTOP AF
RESPONSE AFTER FINAL
EXPEDITED HANDLING REQUESTED

Commissioner for Patents
Alexandria, VA 22313-1450
U.S.A.
Dear Sir:

APPELANT'S BRIEF UNDER 37 C.F.R. 41.37

The following is the Appellant's Brief, submitted under the provisions of 37 C.F.R. 41.37. The fee of $250 that is required by 37 C.F.R. 41.20(b)(2) for filing a brief in support of the appeal is enclosed.

Real Party in Interest

The real party in interest is the applicant, i.e. Vincent So, current address 529 Chapel Street, Ottawa, Ontario, Canada, K1N 8AJ.

Related Appeals and Interferences

There are no related appeals or interferences that will directly affect, be directly affected by, or have a bearing on the present appeal.

Status of the Claims

Claims 1-23 and 34-43 are currently pending in the application. Claims 1-23 and 34-43 stand rejected and the rejection is appealed.

Claims 24-33 are cancelled.

An Appendix containing a copy of the appealed claims is attached hereto.

Status of Amendments

Claims 24-33 were cancelled in an Office Action response filed on January 24, 2007. Claims 35 and 37 were amended in the same Office Action response.

The response of January 24, 2007 was considered by the Examiner, but deemed not to be persuasive, as discussed in detail in the Final Office Action issued by the Examiner dated March 29, 2007.

A response filed on May 29, 2007, which included amendments to claim 40 was considered by the Examiner, but deemed not to be persuasive, as indicated in the Advisory Action issued by the Examiner dated July 11, 2007. In the Advisory Action, the Examiner indicates that for the purposes of appeal, the amendments included in the response filed on May 29, 2007 will not been entered.

Accordingly, it is Applicant's understanding that the claims presently on file correspond to the listing of claims filed in the Office Action response dated January 24, 2007.

Summary of the Claimed Subject Matter

The invention as recited in independent claim 1 relates to "A method of delivering data content from a data content provider to a customer processing platform and controlling use of the data content at the customer processing platform". A flowchart of an embodiment of such a method is shown in Figure 3, and a detailed description of the embodiment is given beginning on Page 18, line 26. A block diagram of a data content delivery system that includes a data content provider video server 10 and a customer processing platform implemented by a download controller 16 that is part of a computer system 14 is shown in Figure 1. A description of the operation of the system shown in Figure 1 is given beginning on page 10, line 17. Figure 4 is a block diagram of another embodiment of a system for delivering data content from content providers 52, 54, 56 to customer processing platforms, which are implemented as download controllers 79, 81 on computer systems 78, 80. The operation of the system shown in Figure 4 is given beginning on page 26, line 22. Control of the use of the data content at the customer processing platform is shown in method steps 41-44 of Figure 3, and the accompanying description beginning on page 19, line 29.

In claim 1, the method is recited to include "encrypting each of a plurality of sections of the data content using a respective one of a plurality of encryption keys to produce a corresponding plurality of encrypted sections". An example of such an encrypting step is described with reference to step 27 of Figure 2 on page 17, line 7 to line 20.

In claim 1, the method is recited to also include "delivering the plurality of encrypted sections to the customer processing platform". Delivery of encrypted sections to customer processing platforms is described with reference to steps 28-30 of Figure 2 on page 17, line 21 to line 31.

In claim 1, the method is recited to also include "delivering to the customer processing platform a plurality of decryption keys corresponding to the plurality of encryption keys, wherein the decryption keys are delivered in a manner such that the customer processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time". Delivery of decryption keys corresponding to the plurality of encryption keys in such a manner is described with reference to Figure steps 41-44 of Figure 3 on page 19, line 29 to page 20, line 7.

Delivering all of the decryption keys to the customer platform in a manner that ensures that the customer processing platform only has simultaneous possession of at most a subset of the decryption keys effectively controls the use of the data content at the customer processing platform. In the embodiment shown in Figure 3, a decryption key for a previous encrypted section is destroyed before the decryption key for the next encrypted section is delivered to the customer processing platform. The timing of the delivery of decryption keys and the destruction of previous keys may vary depending on the specific implementation, as described on page 21, lines 3 to 22.

Claim 2 is dependent on claim 1. Claim 2 recites "wherein delivering to the customer processing platform a plurality of decryption keys comprises: delivering to the customer processing platform a first key of the plurality of decryption keys for a first encrypted section of the plurality of encrypted sections; delivering to the customer processing platform a second key of the plurality of decryption keys for a second encrypted section of the plurality of encrypted sections; and causing the first key to be destroyed at the customer processing platform". As noted above, steps 41 to 44 of Figure 3 and the accompanying description on page 19, line 29 to page 20, line 7, relate to the delivery of a first decryption key for a first encrypted section, and the delivery of a second decryption key for a second encrypted section, once the first decryption key has been destroyed. Also as noted above, page 21, lines 3 to 22 clarify that, in some embodiments, the second decryption key may be delivered before the first key is destroyed, but that the first key is destroyed at least before all of the other decryption keys are obtained by the customer processing platform. Examples of mechanisms for causing the current decryption key to be destroyed are discussed on page 24, lines 5-13. For example, key control software may be delivered to the customer processing platform that destroys decryption keys to prevent the customer processing platform from having simultaneous possession of the entire set of decryption keys. Alternatively, an explicit command may be sent from the data content provider to the customer processing platform to destroy decryption keys.

Claim 3 is dependent on claim 1. Claim 3 recites "wherein delivering to the customer processing platform a plurality of decryption keys comprises: delivering to the customer processing platform a current key of the plurality of decryption keys for a current encrypted section of the plurality of encrypted sections to be processed at the customer processing platform; delivering to the customer processing platform a next key of the plurality of decryption keys for a next encrypted section of the plurality of encrypted sections to be subsequently processed at the customer processing platform upon completion of processing of the current encrypted section; and causing the current key to be destroyed at the customer processing platform". Claim 3 is similar to claim 2, and is supported by the same portions of the specification identified above with reference to claim 2. Claim 3 relates to decryption keys and encrypted sections that are not necessarily the first and second decryption keys and encrypted sections. Delivery of decryption keys and encrypted sections other that the first and second decryption keys and encrypted sections are described with reference to Figure 4 on page 20, lines 8-16.

Claim 4 is dependent on claim 3. Claim 4 recites "wherein delivering to the customer processing platform a next key of the plurality of decryption keys and causing the current key to be destroyed at the customer processing platform are repeated for each of the plurality of encrypted sections to be subsequently processed". Steps 39-44 of Figure 4 of Figure 3 show an example of a method for repeating the delivering and destroying steps of claim 3 for each of the plurality of encrypted sections to be subsequently processed. A detailed description of steps 39-44 of Figure 3 is provided on page 19, line 29 to page 20, line 7, and another description of the destroying of decryption keys in accordance with claim 4 is provided on page 21, lines 3 to 22.

Claim 5 is dependent on claim 3. Claim 5 recites "wherein the current encrypted section is a first one of the plurality of encrypted sections, and wherein delivering to the customer processing platform a next key of the plurality of decryption keys and causing the current key to be destroyed at the customer processing platform are repeated for each of the plurality of encrypted sections following the first encrypted section". As noted above with reference to claim 4, steps 39-44 of Figure 4 of Figure 3 show an example of a method for repeating the delivering and destroying steps of claim 3 for each of the plurality of encrypted sections following the first encrypted section. A detailed description of steps 39-44 of Figure 3 is provided on page 19, line 29 to page 20, line 7. Claim 5 specifies that the current encrypted section is a first one of the plurality of encrypted sections. Page 21, lines 3 to 22, describe the decryption of the first, second and subsequent encrypted section using the first, second and subsequent decryption keys, respectively, in a method in accordance with claim 5.

Claim 6 is dependent on claim 1. Claim 6 recites in part "wherein delivering to the customer processing platform a plurality of decryption keys comprises: providing key control software to the customer processing platform". Key control software is described on page 15, line 28 to page 16, line 5 and on page 24, lines 5-13. Key control software might, for example, be downloaded, stored and executed on the download controller 16 shown in Figure 1, or the download controllers 79, 80 shown in Figure 4. In the embodiment shown in Figure 4, key control software may be downloaded from the content providers 52, 54, 56, as described on page 24, lines 2-4.

Claim 6 also recites "the key control software being adapted to: receive a decryption key for one of the plurality of encrypted sections; complete decryption of the one section; and destroy the decryption key". Operation of an embodiment of key control software is described on page 15, line 28 to page 16, line 5 and on page 24, lines 5-13. The key control software is described beginning on page 15, line 31 as being "configured to receive a key or transmission value for a given section of encrypted data content, to decrypt the given section, and then destroy the key. ... the key control software also preferably deletes any keys for other sections of encrypted data content that are accessible to the customer processing platform." As noted above, decrypting subsequent encrypted sections with subsequent decryption keys and destroying the current decryption key and any subsequent decryption key after decryption of the subsequent encrypted section is shown in steps 39-44 of Figure 3.

Claim 7 is dependent on claim 1. In claim 7, it is recited that the method of claim 1 further comprises "billing a customer for delivery of the encrypted sections, and then billing the customer each time the data content is used at the customer processing platform". A pay-per-view data content delivery and control method is described on page 8, lines 3-7, on page 16, lines 6-12 and with reference to Figure 2 beginning on page 16, line 14. In the flowchart shown in Figure 2, the customer is billed for the delivery of the encrypted data content in step 26. On page 16, lines 6-12 it is explained that, in some embodiments, "a customer is billed first for downloading data content and then for each time keys for the data content are downloaded, to view a movie for example". Because the plurality of decryption keys are delivered in a manner such that the customer processing platform has simultaneous possession of at most a subset of the plurality of decryption keys, the decryption keys that the customer processing platform does not have possession of must be re-downloaded each time the customer wants to use the data content, i.e. to decrypt the encrypted sections.

Claim 8 is dependent on claim 1. Claim 8 recites "wherein the data content is video content or music content, and wherein use of the data content at the customer processing platform comprises decryption and playback of the data content". Video content and music content are described as examples of data content on page 22, lines 16-28, and use of the video or music content is described specifically as decryption and playback of the data content 22, lines 23-28.

Claim 9 is dependent on claim 1. Claim 9 recites "wherein each of the plurality of encryption keys comprises a respective symmetric cryptographic key, and wherein each of the plurality of decryption keys comprises the symmetric cryptographic key of its corresponding encryption key". Symmetric cryptographic keys and their use in embodiments of the present invention are described on page 12, lines 5-11 and on page 14, lines 10-17. On page 12, lines 5-6 it is stated that "[t]he secret decryption key is the same as the secret encryption key in symmetric encryption schemes". On page 14, lines 10-12, it is stated that "symmetric key cryptography involves the same keys for encryption and decryption operations".

Claim 10 is dependent on claim 1. Claim 10 recites that the method of claim 1 further comprises "generating each of the plurality of encryption keys using an identifier associated with the customer processing platform, to thereby generate a plurality of customer processing platform-specific keys". Generating the encryption keys using an identifier associated with the customer processing platform is described beginning on page 14, line 18, which states that "[s]everal options exist for determining customer processing platform-specific keys. Key determination based on unique customer processing platform identifiers is generally preferred so that each customer processing platform has a unique key or set of keys. A network address such as an IP address or hardware identifiers associated with a computer system upon which the customer processing platform is operating are two illustrative examples of possible unique identifiers".

Claim 11 is dependent on claim 10. Claim 11 recites "wherein generating comprises generating each of the plurality of customer processing platform-specific keys using the identifier and a respective key generation seed value." Generating customer processing platform-specific keys using an identifier and a respective key generation seed value is described beginning on page 14, line 26, which states that "[i]n one embodiment, decryption key generation seed values are combined with or transformed using such a unique identifier to generate the decryption keys. Transfer of the key generation seed values to a customer processing platform for corresponding transformation into required decryption keys allows data content decryption to be restricted to a particular computer system or location. Mappings between customer processing platforms and the corresponding keys or seed values are preferably maintained at a data content provider, in a mapping table in memory, for instance".

Claim 12 is dependent on claim 11. Claim 12 recites "wherein delivering to the customer processing platform a plurality of decryption keys comprises delivering the respective key generation seed values". As noted above with reference to claim 11, page 14, lines 28-32 states that "transfer of the key generation seed values to a customer processing platform for corresponding transformation into required decryption keys allows data content decryption to be restricted to a particular computer system or location" (emphasis added). In operation, the customer processing platform generates the decryption keys using the key generation seed values and its identifier.

Claim 13 is dependent on claim 1. Claim 13 recites that the method of claim 1 further comprises: "generating a respective transmission value for each of the plurality of encryption keys using an identifier associated with the customer processing platform, wherein delivering to the customer processing platform a plurality of decryption keys comprises delivering the transmission values". Generating a respective transmission value for each of the plurality of encryption keys using an identifier associated with a customer processing platform is discussed in detail beginning on page 15, line 3, which states that "[a]ccording to another embodiment, a decryption key is transformed at a data content provider using such a unique customer processing platform identifier. In a simple illustrative example of this embodiment, each decryption key A_n required to decrypt downloaded data content is transformed using a network address B associated with a user's computer system to generate a respective transmission value $C_n = A_n - B$." Delivering the transmission values to the customer processing platform is described beginning on page 15, line 10, which states that "[e]ach transmission value is then sent to the customer processing platform for decryption of encrypted blocks of the data content in the manner described herein. The customer processing platform then performs a reverse transformation on the transmission value to recover the decryption key, as $C_n + B = A_n$ in this example."

Claim 14 is dependent on claim 1. Claim 14 recites that the method of claim 1 further comprises: "delivering the plurality of encrypted sections from the customer processing platform to a second customer processing platform; and delivering the plurality of decryption keys from the data content provider to the second customer processing platform, wherein the decryption keys are delivered in a manner such that the second customer processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time". Peer to peer distribution of encrypted data content, i.e. delivering encrypted data content between customer processing platforms, is described with reference to the peer-to-peer network 86 shown in Figure 4, beginning on page 30, line 18, which states that "[i]n another operating mode, the download controllers 79 and 81 download encrypted data content from other sources than the service providers 66, 68, and 70, including other users.

Peer-to-peer communication techniques, represented in FIG. 4 by the peer-to-peer network 86, are commonly used to share files between computer systems. Although data content is available through the service providers 66, 68, and 70, users are also encouraged to share encrypted data content with other users. For example, after encrypted data content is downloaded to the computer system 78 from the service provider 68, the computer system 78 effectively becomes another distribution point for the encrypted data content. Downloaded encrypted data content is then available to the computer system 80 and other computer systems through the peer-to-peer network 86. On-line file sharing services are among the most common means for sharing data between computer systems. However, it should be appreciated that downloaded encrypted data may be shared using other distribution channels, including but not limited to email and such portable storage media as CDs, DVDs, diskettes, and memory cards.

Thus, the peer-to-peer network 86 is shown in FIG. 4 as one illustrative example of the many possible mechanisms for sharing encrypted data content between computer systems and users" (emphasis added).

Claim 15 depends on claim 1. Claim 15 recites "[a] computer-readable medium storing instructions which, when executed by a processor at a data content provider, perform a method according to claim 1". On page 22, line 29 it is stated that in some embodiments, "[t]he foregoing systems and methods are implemented as a computer readable medium containing software code executable by a processing platform in an embodiment of the invention".

Claim 16 is and independent claim that relates to "[a] method of receiving and controlling playback of data content at a customer processing platform". Figure 3 illustrates a flowchart of a method that includes receiving and controlling playback of data content at a customer processing platform. Receiving encrypted data content at a customer processing platform is also described with reference to Figure 1, beginning on page 11, line 23 and with reference to Figure 4, beginning on page 26, line 22. Controlling playback of data content at a customer processing platform is described beginning on page 21, line 23. As noted above with reference to Figure 1, a customer processing platform may, for example, be implemented as part of the computer system 78, 80 shown in Figure 4, or the computer system 14 shown in Figure 1.

Claim 16 recites that the method comprises: "receiving over a communications medium a plurality of encrypted sections of data content, each of which has been encrypted using a respective encryption key". As noted above with reference to claim 14, encrypted data content may be delivered by a wide variety of delivery mechanisms: broadcast communications, direct download, on CDs, DVDs, diskettes, memory cards, e-mail, peer-to-peer file sharing, etc. Accordingly, the communications medium may be any medium by which the encrypted data content can be delivered/communicated to the customer processing platform. Encryption of sections of data content using respective encryption keys is described, for example, with reference to step 27 of the flowchart of Figure 2 beginning on page 17, line 7, which states that "[a]t 27, encryption is applied to each of a plurality of sections of each video to be downloaded. For example, if a video is to be downloaded in four sections, then encryption is applied to each of the four sections in step 27".

In claim 16, the method is recited to also include "for each encrypted section: receiving a decryption key in respect of the encrypted section; decrypting and playing back the encrypted section using the decryption key; and destroying the decryption key after completing playback of the encrypted section". As noted above, steps 41 to 44 of Figure 3 and the accompanying description on page 19, line 29 to page 20, line 7, relate to the delivery of a first decryption key for a first encrypted section, and the delivery of a second decryption key for a second encrypted section, once the first decryption key has been destroyed. Also as noted above, page 21, lines 3 to 22 clarify that, in some embodiments, the second decryption key may be delivered before the first key is destroyed, but that the first key is destroyed at least before all of the other decryption keys are obtained by the customer processing platform.

Claim 17 is dependent on claim 16. Claim 17 recites that the method of claim 16 further comprises "for each encrypted section: destroying decrypted data content at the customer processing platform after completing playback of the encrypted section". Page 22, lines 7-12 state that in some embodiments, "a different key is transmitted to the customer at an appropriate time to enable the customer to use the next section of the data content, preferably without any interruption, and the first key and any related decrypted data content from the first section is destroyed at the customer's computer system" (emphasis added).

Claim 18 is dependent on claim 16. Claim 18 recites "wherein the communications medium is the public Internet". Delivery of encrypted data content via the Internet is specifically discussed with reference to Figure 1 on page 8, lines 10-12 and with reference to Figure 4 on page 26, lines 1-4.

Claim 19 is dependent on claim 16. Claim 19 recites "wherein, for each encrypted section, the encryption key is the same as the decryption key". As noted above with reference to claim 9, symmetric encryption/decryption systems involve the use of the same key for encryption and decryption. On page 12, lines 5-6 it is stated that "[t]he secret decryption key is the same as the secret encryption key in symmetric encryption schemes". On page 14, lines 10-12, it is stated that "symmetric key cryptography involves the same keys for encryption and decryption operations".

Claim 20 is dependent on claim 16. Claim 20 recites "wherein receiving the plurality of encrypted sections of the data content comprises receiving the plurality of encrypted sections of the data content from another customer processing platform". As noted above with reference to claim 14, peer to peer distribution of encrypted data content, i.e. delivering encrypted data content between customer processing platforms, is described with reference to the peer-to-peer network 86 shown in Figure 4, beginning on page 30, line 18, which states that "[i]n another operating mode, the download controllers 79 and 81 download encrypted data content from other sources than the service providers 66, 68, and 70, including other users" (emphasis added).

Claim 21 is dependent on claim 16. Claim 21 recites "[a] computer-readable medium storing instructions which, when executed by a customer processing platform, perform a method according to claim 16". As noted above with reference to claim 15, page 22, line 29 states that in some embodiments, "[t]he foregoing systems and methods are implemented as a computer readable medium containing software code executable by a processing platform in an embodiment of the invention".

Claim 22 is dependent on claim 16. Claim 22 recites "" "wherein each encryption key comprises a respective customer processing platform-specific key which is determined based on an IP address of the customer processing platform". As noted above with reference to claim 10, generating the encryption keys using an identifier associated with the customer processing platform is described beginning on page 14, line 18, which states that "[s]everal options exist for determining customer processing platform-specific keys. Key determination based on unique customer processing platform identifiers is generally preferred so that each customer processing platform has a unique key or set of keys. A network address such as an IP address or hardware identifiers associated with a computer system upon which the customer processing platform is operating are two illustrative examples of possible unique identifiers".

Claim 23 is dependent on claim 16. Claim 23 recites "wherein receiving each decryption key comprises receiving a transmission value that is determined based on the decryption key and a hardware identifier associated with the customer processing platform, further comprising, for each encrypted section: recovering the decryption key from the transmission value". As noted above with reference to claim 22, a hardware identifier is one example of a unique identifier, and as noted above with reference to claim 13, generating a respective transmission value for each of the plurality of encryption keys using an identifier associated with a customer processing platform is discussed in detail beginning on page 15, line 3, which states that "[a]ccording to another embodiment, a decryption key is transformed at a data content provider using such a unique customer processing platform identifier. In a simple illustrative example of this embodiment, each decryption key A_n required to decrypt downloaded data content is transformed using a network address B associated with a user's computer system to generate a respective transmission value $C_n = A_n - B$." Reception of the transmission values at the customer processing platform is described beginning on page 15, line 10, which states that "[e]ach transmission value is then sent to the customer processing platform for decryption of encrypted blocks of the data content in the manner described herein. The customer processing platform then performs a reverse transformation on the transmission value to recover the decryption key, as $C_n + B = A_n$ in this example" (emphasis added).

Claim 34 is an independent claim that relates to "[a] method for controlling use of encrypted data content downloaded to a customer data content processing device". As noted above with reference to claim 1, controlling use of encrypted data content is described beginning on page 19, line 29 with reference to the method steps 41-44 of Figure 3. Controlling use of encrypted data content may involve destruction of decryption keys and/or destruction of decrypted data content, as described, for example, on page 22, lines 7-12, which states that in some embodiments, "a different key is transmitted to the customer at an appropriate time to enable the customer to use the next section of the data content, preferably without any interruption, and the first key and any related decrypted data content from the first section is destroyed at the customer's computer system" (emphasis added).

A customer data content processing device may, for example, be implemented by the download controller 16 that is part of the computer system 14 shown in Figure 1, or as one of the download controllers 79, 81 that are part of the computer system 78, 80 shown in Figure 4.

In claim 34, it is recited that the method comprises: "receiving a request comprising customer verification information from a customer data content processing device".

With reference to Figure 1, it is stated beginning on page 10, line 26 that "[a]ccording to one embodiment, the video download controller 16 includes a user or customer interface that facilitates the exchange of customer verification information and subsequent rental selection information between a customer, at the computer system 14, and the video server 10. Customer verification information includes such information as a network address of the computer system 14, a customer email address, or a customer or account identification number. Customer verification information is also stored at the video server 10 for all properly registered customers or subscribers. It should be appreciated that the customer verification information may include more than one type of customer-related information. For example, access to the video server 10 by any customer may be restricted to particular computers or locations where customer verification information includes both a customer ID and a network address. In this case, the video server 10 grants access to its data content only if a customer establishes a connection from a predetermined network address. However, more common password-based access control is also contemplated for the video server 10. In other embodiments, the network address of the computer system 14 is transferred to the video server 10 as a destination address for file downloading as described in further detail below, and access control is based on other customer verification information provided to the video server 10" (emphasis added).

In claim 34, it is also recited that the method includes "comparing the customer verification information with corresponding stored customer information; and where the customer verification information is consistent with the stored customer verification information: billing a usage charge to an account of the customer; transmitting to the customer data content processing device a digital key to decrypt a current portion of the encrypted data content; and for each subsequent portion of the encrypted data: transmitting to the customer data content processing device a different key to decrypt the subsequent portion of the encrypted data; and causing a key for a preceding portion of the encrypted data to be deleted from the customer data content processing device".

Comparing customer verification information with corresponding stored customer information is described beginning on page 18, line 15, which states that "[t]he data content provider server compares the customer verification information with locally stored corresponding customer verification information, and in the event that the locally stored and transmitted customer verification information match, the order information is processed. Ordered data content is encrypted with a set of digital keys such that different sections of the data content are encrypted with different keys. In a per-download billing model, a customer account is billed either at download time or upon confirmation that encrypted data content has been received".

Figure 3 illustrates a method of billing a user charge to a customer account (step 36) and transmitting to the customer data content processing device a digital key to decrypt a current portion of the encrypted data content (step 37); and for each subsequent portion of the encrypted data: transmitting to the customer data content processing device a different key to decrypt the subsequent portion of the encrypted data (step 41); and causing a key for a preceding portion of the encrypted data to be destroyed (step 44).

Claim 35 is an independent claim that relates to "[a] computer readable medium storing software code executable by a processing platform". As noted above with reference to claims 15 and 21, page 22, line 29 states that in some embodiments, "[t]he foregoing systems and methods are implemented as a computer readable medium containing software code executable by a processing platform in an embodiment of the invention". The processing platform may, for example, be implemented by the download controller 16 that is part of the computer system 14 shown in Figure 1, or as one of the download controllers 79, 81 that are part of the computer system 78, 80 shown in Figure 4.

In claim 35, the software code is recited to include: "first software code for coordinating downloading a plurality of sections of data content each encrypted with a respective one of a plurality of encryption keys to a customer computer system from a data content service provider system or another customer computer system". Coordinating the downloading of a plurality of sections of data content each encrypted with a respective one of a plurality of encryption keys is described in detail with reference to the download controller 16 of the computer system 14 shown in Figure 1 and the download controllers 79, 81 of the computer system 78, 80 shown in Figure 4, beginning on page 13, line 28 and on page 30, line 13, respectively. The video server 10 shown in Figure 1 may be provided by a data content service provider. Figure 4 illustrates one example of a system for downloading encrypted data content from content providers 52, 54, 56 or for sharing encrypted data content between customer computer systems 78, 80 via a peer-to-peer network 86. As noted above, beginning on page 30, line 18, it is stated that "[i]n another operating mode, the download controllers 79 and 81 download encrypted data content from other sources than the service providers 66, 68, and 70, including other users. ... For example, after encrypted data content is downloaded to the computer system 78 from the service provider 68, the computer system 78 effectively becomes another distribution point for the encrypted data content. Downloaded encrypted data content is then available to the computer system 80 and other computer systems through the peer-to-peer network 86. ... However, it should be appreciated that downloaded encrypted data may be shared using other distribution channels, including but not limited to email and such portable storage media as CDs, DVDs, diskettes, and memory cards. Thus, the peer-to-peer network 86 is shown in FIG. 4 as one illustrative example of the many possible mechanisms for sharing encrypted data content between computer systems and users" (emphasis added).

In claim 35, it is also recited that the software code includes "second software code for establishing a connection with the data content service provider system to obtain permission to use the data content, and for using the data content where permission is obtained from the data content service provider system by receiving a corresponding one of a plurality of decryption keys for each encrypted section of data content and decrypting the encrypted section using the corresponding one of the plurality of decryption keys such that the processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time".

Software that is executed, for example, by the download controller 16 in Figure 1 or the download controllers 79, 81 shown in Figure 4, is described beginning on page 33, line 1, which states that "[t]he required software program may be incorporated in download controller software, which may itself be downloaded, or a separate software component that is downloaded either with a first data content download or the first time that a user requests to use any data content. The software program preferably requires a customer to establish a connection with a service provider and obtain keys or permission to use the data content. The customer may be required to enter certain information in order to gain permission. After any such information has been verified, permission is granted and a charge is billed to the customer's account or credit card. The customer may then begin to use the data content. During use of the data content, the customer preferably stays connected to the service provider, and from time to time further permissions from the service provider are required for continued use of the data content" (emphasis added). Figure 3, and the accompanying description provided beginning on page 19, line 29 describe receiving a corresponding one of a plurality of decryption keys (step 37) for each encrypted section of data content and decrypting the encrypted section using the corresponding one of the plurality of decryption keys (step 38) such that the processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time (destroying current key after the current section is finished; step 44). As noted above, the decrypted data content may also be destroyed.

Claim 36 is dependent on claim 35. Claim 36 recites "wherein the second software code obtains further permissions from the data content service provider system to continue using the data content". As noted above with reference to claim 35, page 33, lines 12-16 state that "[d]uring use of the data content, the customer preferably stays connected to the service provider, and from time to time further permissions from the service provider are required for continued use of the data content" (emphasis added).

Claim 37 is an independent claim that relates to "[a] signal embodied on a transmission medium containing software code executable by a processing platform". Such a signal is described beginning on page 23, line 12, which states that "[i]n embodiments that support download of this software itself to a processing platform, the invention provides a signal embodied on a transmission medium containing software code executable by the processing platform".

The software code recited by claim 37 is identical to the software code recited in claim 36, and is supported in the same portions of the specification as identified above with reference to claim 36.

Claim 38 is an independent claim that is related to "[a] system for delivering data content from a data content provider to a customer processing platform and controlling use of the data content at the customer processing platform". A block diagram of a data content delivery system that includes a data content provider video server 10 and a customer processing platform implemented by a download controller 16 that is part of a computer system 14 is shown in Figure 1. A description of the operation of the system shown in Figure 1 is given beginning on page 10, line 17. Figure 4 is a block diagram of another embodiment of a system for delivering data content from content providers 52, 54, 56 to customer processing platforms, which are implemented as download controllers 79, 81 on computer systems 78, 80. The operation of the system shown in Figure 4 is given beginning on page 26, line 22. Control of the use of the data content at the customer processing platform is shown in method steps 41-44 of Figure 3, and the accompanying description beginning on page 19, line 29.

In claim 38, the recited system includes "means for encrypting each of a plurality of sections of the data content using a respective one of a plurality of encryption keys to produce a corresponding plurality of encrypted sections". The video server 10 shown in Figure 1 is an example of a means for encrypting each of a plurality of sections of data content. Beginning on page 11, line 24, it is stated that "the video server 10 encrypts selected data content, using any known encryption algorithm and either a public or secret encryption key, and the encrypted data content is delivered to the customer using the data network 12". Beginning on page 12, line 21 it is stated that "[i]n a preferred embodiment, encrypted data content is protected by a set of cryptographic keys. Each key can only decrypt a particular section of the encrypted data content. Key distribution is controlled such that a customer is in possession of less than the entire set of keys, preferably only a single key, at any time." The data content server 64 shown in Figure 4 is described as another example of a means for encrypting each of a plurality of sections of the data content using a respective one of a plurality of encryption keys. Beginning on page 29, line 1, it is stated that "[i]n a particularly preferred embodiment, the data content server 64 segments and encrypts any received data content ... and locally stores the encrypted data content" (emphasis added).

In claim 38, it is also recited that the system includes "means for delivering the plurality of encrypted sections to the customer processing platform". With reference to Figure 1, means for delivering encrypted content to a customer processing platform is described as being implemented by the video server 10, which is connected to an Internet service provider 20 through a data network 12. The customer computer system 14 can download encrypted data content from the video server 10 through the Internet service provider 20 using the download controller 16, and store the encrypted data content in the storage 15. Beginning on page 9, line 3, it is stated that "[t]he video server 10 is established at a location on the data network 12 where customers may gain access to its video content. In one embodiment, the location is a website, which includes a number of web pages. These web pages preferably require a customer to enter authorization information in order to gain further access, and may also include further information about the content available through the video server 10. In another embodiment, the video server 10 includes a database that stores video content and possibly user information associated with users that are authorized for access to the stored video content.

The computer system 14 is preferably a personal computer, and is capable of establishing a connection to the video server 10 through the service provider 20. However, it is to be understood that any appropriate mechanism of establishing the connection to the video server 10 may be employed. The storage device 15 is configured to store content downloaded to the computer system 14 as described in further detail below. For large file downloads such as movie files, a hard disk drive or other high capacity storage device is preferred, although the storage device 15 may also or instead comprise one or more of a compact disk device, a digital video disk device, a solid-state memory, and other types of memory systems. It will be apparent to those skilled in the art that the memory device 15 need not be dedicated to storing downloaded content, and is typically accessible to other components of the computer system 14 in addition to the video download controller 16".

Claim 38 also recites "means for delivering to the customer processing platform a plurality of decryption keys corresponding to the plurality of encryption keys, wherein the decryption keys are delivered in a manner such that the customer processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time." Beginning on page 12, line 12, it is stated that "Thus, to use the data content, the customer must first obtain the required secret decryption key. In one embodiment, the customer requests the decryption key from the video server 10. After the video server 10 has authenticated the user, by checking a network address of a computer system from which a decryption key request is received, a password for a customer account, a digital signature on a key request, or some combination thereof, for example, the appropriate key is identified and transmitted to the customer in real time.

In a preferred embodiment, encrypted data content is protected by a set of cryptographic keys. Each key can only decrypt a particular section of the encrypted data content. Key distribution is controlled such that a customer is in possession of less than the entire set of keys, preferably only a single key, at any time. When a decryption key for a section of the encrypted data content is sent to a customer, the video download controller 16 deletes one or more keys, as well as decrypted data content, for other sections of the encrypted data content. Storage of keys and decrypted data content at a customer's computer system is also preferably controlled to prevent storage of any keys or decrypted content to permanent memory. These measures render copying of data content for reproduction or access after a rental or subscription period has expired more difficult" (emphasis added).

Claim 39 is dependent on claim 38. Claim 38 recites "wherein the customer processing platform comprises: means for requesting the data content to be delivered to the customer processing platform; means for receiving the plurality of encrypted sections; means for receiving, for each encrypted section, the decryption key in respect of the encrypted section; means for decrypting and playing back the encrypted section using the decryption key; and means for destroying the decryption key, after completing playback of the encrypted section".

On page 13, lines 28-30, it is stated that "[i]n a more general sense, the video download controller 16 may be considered as one specific embodiment of a customer processing platform. Beginning on page 10, line 1, the video download controller 16 is described as preferably comprising "a software module or program running on the computer system 14. In a preferred embodiment, the video download controller 16 is a plug-in adapted to run together with a browser on the computer system 14. In other embodiments, the video download controller 16 is any appropriate software installed on the computer system 14 which is capable of controlling the download and subsequent playing of data content, video content in FIG. 1. A software-based video download controller 16 may itself be downloaded onto the computer system 14, such as when a user first subscribes to a video rental service supported by the video server 10" (emphasis added).

Beginning on page 13, line 4, it is stated that "[t]he video download controller 16 also controls playback of downloaded video content. Where multiple-key protection is implemented, the video download controller 16 preferably requests each decryption key as it is needed to play back sequential sections of encrypted video. To view each section, another digital key is downloaded from the video server 10, and the digital key and any remaining decrypted video content that may have been temporarily stored during playback for the previous section are destroyed, by deletion from memory, for example".

Claim 40 is an independent claim related to "[a] data content distribution system". A data content distribution system is illustrated in Figure 1, which is described in detail beginning on page 8, line 8, and in Figure 4, which is described in detail beginning on page 25, line 21.

In claim 40, the recited system includes "a data content server configured to receive download requests and permission requests for data content, to encrypt a plurality of sections of requested data content using respective encryption keys to thereby generate a plurality of encrypted sections and to transmit the encrypted sections of the data content in response to a received download request for the data content, and to transmit each of a plurality of decryption keys respectively corresponding to the encryption keys in response to a permission request for the data content". Such a data content server is illustrated by way of example in the video server 10 shown in Figure 1, and the combination of the data content server 64 shown in Figure 4, although peer-to-peer sharing of encrypted data content is also contemplated.

With reference to Figure 4, and, as noted above with reference to claim 39, page 29, lines 1-4 recite that "[i]n a particularly preferred embodiment, the data content server 64 segments and encrypts any received data content as described above and locally stores the encrypted data content".

In some embodiments, some of the functions of the data content server 64 may be transferred to the service providers. For example, as described beginning on page 29, line 7, "The service providers 66, 68, and 70 communicate with the data content server 64 to obtain encrypted data content and the decryption keys required to decrypt the encrypted data content. Communications over the links 72, 74, and 76 are preferably secure, particularly where actual decryption keys are transferred from the data content server 64. Any of the key protection techniques described above may be applied to key transfer between the data content server 64 and the service providers 66, 68, and 70. However, the service providers are preferably provided with the full set of decryption keys required to decrypt encrypted data content, as well as any other information, such as a custom software application, module, or plug-in, required by a customer to use the data content. Each service provider 66, 68, and 70 is thereby enabled to respond to consumer requests to download and/or use data content, offloading such functions from the data content server 64".

Claim 40 also recites "a data content download controller configured to generate download requests, to receive encrypted sections of data content in response to download requests, to generate permission requests when downloaded data content is to be used, and for each encrypted section of data content to be used, to receive a corresponding one of the plurality of decryption keys, and to decrypt the encrypted section using the corresponding one of the plurality of decryption keys". Such a data content download controller is illustrated, by way of example, by the video download controller 16 shown in Figure 1, and described beginning on page 10, line 1, and by the download controllers 79, 81 shown in Figure 4, and described beginning on page 30, line 13.

Claim 41 is dependent on claim 40. Claim 41 recites "[t]he system of claim 40, comprising a data network connecting the data content server and the data content download controller". An example of such a data network is provided by the data network 12 shown in Figure 1. In addition, with reference to the connections 72, 74 and 76 shown in Figure 4, page 26, lines 1-3 states that "[i]n many implementations, at least some of these connections are made through one or more communication networks, including the Internet, and intermediate systems and servers supporting such network connections".

Claim 42 is dependent on claim 41. Claim 42 recites that the system further comprises "a plurality of data content download controllers connected to the data network". Figure 4 illustrates an example of a data content delivery system in which a plurality of download controllers 79, 81 are connected through their service providers 68, 80 and the data network that supports the network connections 74, 76 to the data content server 64.

Claim 43 is dependent on claim 42. Claim 43 recites "wherein each of the plurality of data content download controllers is implemented in conjunction with a respective customer computer system and is further configured to download encrypted sections of data content from other customer computer systems". Figure 4 illustrates a system in which the download controllers 79, 81 are implemented in conjunction with the computer systems 78, 80, respectively, and the computer system 78, 80 are able to share encrypted data content using, for example, the peer-to-peer network 86. With reference to Figure 4, beginning on page 30, line 22, it is stated that "peer-to-peer communication techniques, represented in FIG. 4 by the peer-to-peer network 86, are commonly used to share files between computer systems. Although data content is available through the service providers 66, 68, and 70, users are also encouraged to share encrypted data content with other users. For example, after encrypted data content is downloaded to the computer system 78 from the service provider 68, the computer system 78 effectively becomes another distribution point for the encrypted data content. Downloaded encrypted data content is then available to the computer system 80 and other computer systems through the peer-to-peer network 86. On-line file sharing services are among the most common means for sharing data between computer systems. However, it should be appreciated that downloaded encrypted data may be shared using other distribution channels, including but not limited to email and such portable storage media as CDs, DVDs, diskettes, and memory cards. Thus, the peer-to-peer network 86 is shown in FIG. 4 as one illustrative example of the many possible mechanisms for sharing encrypted data content between computer systems and users" (emphasis added).

Grounds of Rejection to be Reviewed on Appeal

The issues which are hereby presented for review are as follows:

1. whether claims 1, 7-13, 15 and 35-38 are unpatentable under 35 U.S.C. 102(e) as being anticipated by Peterka et al. (U.S. Patent Application Publication No. 2002/0170053);

2. whether claims 2-6, 16-19, 21-23 and 39 are unpatentable under 35 U.S.C. 103(a) over Peterka et al. in view of Stirling et al. (U.S. Patent Application Publication No. 2003/0223583);

3. whether claim 14 is unpatentable under 35 U.S.C. 103(a) over Peterka et al. in view of Ginter et al. (U.S. Patent Application Publication No. 2006/0218651);

4. whether claim 20 is unpatentable under 35 U.S.C. 103(a) over Peterka et al. in view of Stirling et al. and further in view of Ginter et al.; and

5. whether claim 34 is unpatentable under 35 U.S.C. 103(a) over Peterka et al. in view of Negawa (U.S. Patent Application Publication No. 2003/0046539).

Arguments

1. Whether claims 1, 7-13, 15 and 35-38 are unpatentable under 35 U.S.C. 102(e) as being anticipated by Peterka et al. (U.S. Patent Application Publication No. 2002/0170053).

Controlling case law has frequently addressed rejections under 35 U.S.C. § 102. "For a prior art reference to anticipate in terms of 35 U.S.C. Section 102, every element of the claimed invention must be identically shown in a single reference." *Diversitech Corp. v. Century Steps, Inc.*, 850 F.2d 675, 677, 7 U.S.P.Q.2d 1315, 1317 (Fed. Cir. 1988; emphasis added). The disclosed elements must be arranged as in the claim under review. See Lindemann Machinefabrik v. American hoist & Derrick Co., 730 F.2d 1452, 1458, 221 U.S.P.Q. 481, 485 (Fed. Cir. 1984). If any claim, element, or step is absent from the reference that is being relied upon, there is no anticipation. *Kloster Speedsteel AB v. Crucible, Inc.*, 793 F.2d 1565, 230

U.S.P.Q. 81 (Fed. Cir. 1986; emphasis added). The following analysis of the present rejections is respectfully offered with guidance from the foregoing controlling case law decisions.

In paragraph 3 on page 10 of the Final Office Action dated March 29, 2007, claims 1, 7-13, 15, 35-37, 38 and 40-42 are rejected under 35 U.S.C. 102(e) as being anticipated by Peterka et al. (U.S. Patent Application Publication No. 2002/0170053).

Applicant respectfully submits that Peterka et al. fails to teach or fairly suggest key limitations of independent claims 1, 35, 37 and 38, and therefore Peterka et al. cannot be found to anticipate the present invention given the rulings in *Diversitech Corp. v. Century Steps, Inc.* and *Kloster Speedsteel AB v. Crucible, Inc.* Specifically, Applicant respectfully submits that Peterka et al. fails to teach or even suggest "delivering to the customer processing platform a plurality of decryption keys corresponding to the plurality of encryption keys, wherein the decryption keys are delivered in a manner such that the customer processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time", as recited in independent claim 1, and as similarly recited in independent claims 35, 37 and 38.

Peterka et al. describes a method for distributing encrypted data content which uses a hierarchy of encryption keys to provide for flexible billing options. Specifically, Peterka et al. describes a Pay-By-Time (PBT) billing option (See [0048]) in which a program is segmented into a plurality of program segments. The actual data of each respective program segment is then encrypted with at least one respective content key (CK). The respective content keys are then each encrypted with a respective program segment key (PSK). When a consumer wishes to join a multicast of the program, the consumer contacts an Origin Content Server (OCS) to begin receiving PSKs. The PSKs are distributed to the consumer in a multicast in which the PSKs are encrypted with the consumer's unique key (UK). In order to actually view a program segment, the consumer must first decrypt the PSK corresponding to that program segment with the consumer's UK, then use that decrypted PSK to decrypt the CK corresponding to that program segment and then finally decrypt that program segment with the decrypted CK. In the Pay-By-Time billing method, the consumer must continue to request each new PSK in order to continue viewing the program, i.e. to continue decrypting program segments. Peterka also teaches that the content key for a future program segment may be encrypted with not only the

PSK corresponding to the future program segment, but also with an old PSK of an old program segment. "Thus, if a user has not yet received a new program segment key, the content key can be obtained by utilizing the old program segment key." (see [0109] and Figure 9). Furthermore, Peterka et al. teaches that the content keys are maintained by the consumers, for possible use in later decryption. For example, Peterka describes a signalling method in which "a predetermined bit can be used to indicate if an **old or current content key should be used as opposed to a new content key** which has recently been distributed to the client." (see [0119]; emphasis added)

On pages 11 of the Final Office Action dated March 29, 2007, the Examiner has alleged, in support of his rejection of claims 1, 15 and 38, that Figure 7 and paragraphs [0080], [0082], [0093] and [0102] of Peterka et al. disclose the following feature of claims 1, 15 and 38:

"delivering to the customer processing platform a plurality of decryption keys corresponding to the plurality of encryption keys, wherein the decryption keys are delivered in a manner such that the customer processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time."

The Examiner has further stated that Peterka et al. teaches that the "client has possession of program segment key and the next key ... as well as content keys 0, 1, 2, 3, 4, ...". However, it is respectfully submitted that Peterka et al. does not disclose the above feature, and that the portions of Peterka et al. that the Examiner asserts teach that the "client has possession of program segment key and the next key" merely teach that a current program segment key and a subsequent program segment key are made available to the client at any one given time. It is respectfully submitted that simply making available only a subset of the PSKs at any given time does not guarantee that the client only has simultaneous possession of at most a subset of the PSKs. Accordingly, there is no suggestion in Peterka et al. that if all of the decryption keys have been delivered to the client, the client only has simultaneous possession of at most a subset of the plurality of decryption keys. In fact, the Examiner's own admission that the "client has possession of program segment key and the next key … **as well as the content keys 0, 1, 2, 3, 4, …**" (emphasis added), illustrates that according to Peterka et al., the client has simultaneous possession of all of the content keys once all of the content keys have been received by the client.

In contrast, embodiments of the present invention prevent a client from simultaneously having all of the encrypted content and all of the decryption keys necessary to decrypt the encrypted content. Peterka et al. does not provide this same anti-piracy functionality.

In view of the foregoing, it is respectfully submitted that Peterka et al. fails to teach all of the limitations of independent claims 1 and 38.

With regard to the Examiner's novelty rejection of independent claims 35 and 37, it is respectfully submitted that independent claims 35 and 37 share the same distinguishing limitation of claims 1 and 38 identified above, and therefore distinguish over the teachings of Peterka et al. for at least the same reasons. Applicant further notes that this limitation was added in independent claim 40 in the amendment submitted in response to the Final Office Action, which the Examiner has not entered for the purpose of this appeal.

By virtue of their claim dependencies on one of the independent claims, it is respectfully submitted that dependent claims 7-13, 15 and 36 distinguish over Peterka et al. for at least the same reasons.

It is further submitted that dependent claim 7 recites an additional distinguishing feature over Peterka et al. Specifically, it is respectfully submitted that Peterka et al. fails to teach the following limitation of claim 7:

"billing a customer for delivery of the encrypted sections, and then billing the customer each time the data content is used at the customer processing platform".

The Examiner has pointed to Figures 8 and 9 of Peterka et al. in support of the rejection of claim 7. Figures 8 and 9 of Peterka et al. illustrate encrypted data content distribution methods that include: receiving a request for a cryptographic key from a client; logging the request for the key; logging a segment of the program content for which the key can be used; distributing one or more decryption keys; **distributing program content for decryption by the client utilizing the key; and billing the client based upon log entry(ies).** Therefore, according to Figures 8 and 9 of Peterka et al., and Peterka et al. as a whole, a client must request the cryptographic key **and download the program content again** each time the client wishes to use the data content. According to the teachings of Peterka et al., the client is only billed once the client has re-downloaded the key and the program content, which is completely different than "billing a customer for delivery of the encrypted sections, and then billing the customer each time the data content is used at the customer processing platform", as recited in claim 7.

In view of the fact that Peterka et al. fails to teach a key limitation of the claims, and also fails to identically show every element of the claimed invention, as is required to find that a prior art reference anticipates under 35 U.S.C. § 102, given the rulings in *Kloster Speedsteel AB v. Crucible, Inc.* and *Diversitech Corp. v. Century Steps, Inc.* respectively, it is respectfully submitted that claims 1, 7-13, 15 and 35-38 are novel and inventive over Peterka et al., thus constituting an error in the rejection of the appealed claims.

2. Whether claims 2-6, 16-19, 21-23 and 39 are unpatentable under 35 U.S.C. 103(a) over Peterka et al. in view of Stirling et al. (U.S. Patent Application Publication No. 2003/0223583).

In paragraph 4 on page 15 of the Final Office Action dated March 29, 2007, the Examiner has rejected claims 2-6, 16-19, 21-23 and 39 under 35 U.S.C. § 103(a) as being unpatentable over Peterka et al. in view of Stirling et al. (U.S. Patent Application Publication No. 2003/0223583 A1). It is respectfully submitted that the Examiner has failed to satisfy the requirements for a finding of obviousness recently articulated by the U.S. Supreme Court in its decision in ***KSR Int'l v. Teleflex, Inc.,*** *No. 04-1350, slip op. at 14 (U.S., Apr. 30, 2007).* Accordingly, as a matter of law, the rejection of the claims cannot stand and must be rescinded.

Law

The United States Supreme Court visited the manner by which "obviousness" under 35 U.S.C. §103 is to be interpreted in the case of ***KSR Int'l v. Teleflex, Inc.,*** *No. 04-1350, slip op. at 14 (U.S., Apr. 30, 2007).* As the Court noted in KSR, once the scope of the prior art is ascertained, the content of the prior art must be properly combined. An obviousness inquiry requires review of a number of factors, including the background knowledge possessed by a person having ordinary skill in the art, to determine whether there was an apparent reason to combine the elements of the prior art in the fashion claimed by the present invention. For the Patent Office to properly combine references in support of an obviousness rejection, the Patent Office must identify a reason why a person of ordinary skill in the art would have sought to combine the respective teachings of the applied references. Id. at 15. Even if the Patent Office is able to articulate and support a suggestion to combine the references, it is impermissible to pick and choose elements from the prior art while using the application as a template. ***In re Fine,*** 837 F.3d 1071 (Fed. Cir. 1988). It is respectfully submitted that the 35 U.S.C. §103(a) rejection is deficient for its failure to comply with the U.S. Supreme Court's requirements recently articulated in ***KSR***.

Prima Facie Obviousness Threshold

MPEP 2142 explains the procedural tool of the *prima facie* obviousness threshold, i.e. the applicant does not bear the burden of addressing substantive issues of obviousness (such as secondary considerations) until the examiner makes the prima facie case. A *prima facie* case requires (1) the all elements be taught in the cited reference or references when combined; (2) reasonable expectation of success; and (3) motivation to combine the cited references. 1 and 2 remain irrespective of KSR. The May 3, 2007 memo from Margaret Focarino dealing with the KSR decision states that (3) remains a requirement. More specifically, KSR requires that there be a reason why a person of ordinary skill in the art would have combined the references, and the Focarino memo requires the Examiner to provide such a reason during prosecution.

To begin, Applicant respectfully submits that a first criterion required to establish a case of *prima facie* obviousness has not been satisfied. That is, the prior art references do not teach all of the claimed features.

The Examiner has pointed to paragraph [0080] of Stirling et al. in support of the rejection of claims 2-6 under 35 U.S.C. § 103(a). Paragraph [0080] of Stirling et al. recites a first layer of security in a secure data content delivery system, in which a key management and distribution system is based on constructive key management. An architecture where the key is constructed from multiple components, tokens, keys and hardware. Paragraph [0080] of Stirling et al. refers to one such exemplary product available from TECSEC called Constructive Key Management (CKM) Software. Paragraph [0080] of Stirling et al. is reproduced below.

[0080] The first layer can utilize a key management and distribution system based on constructive key management, an architecture where the key is constructed from multiple components, token, keys, hardware. One suitable exemplary product is Constructive Key Management (CKM) software by TECSEC. The CKM server software is installed at the NOC and at the exhibitor's play out servers. **The CKM software allows the NOC to create authorization tokens for distribution to digital production facilities and intended exhibitor systems. Once the tokens are received at the clients, authorized users (digital production facilities and exhibitors play out servers) can encrypt or decrypt the digital content. The clients CKM software agents will construct (create) a key when needed for encryption or decryption and destroy the key when no longer needed by the encryption/decryption engine.**(emphasis added)

The Examiner appears to be relying on the statement that "[t]he client CKM software agents will construct (create) a key when needed for encryption or decryption and destroy the key when no longer needed by the encryption/decryption engine" to support the assertion that Stirling et al. teaches destroying a decryption key when it is no longer needed. However, the CKM software at the server side (Network Operation Center) creates authorization tokens for distribution to digital production facilities and intended exhibitor systems. The tokens allow content to be encrypted and decrypted at client sites. The client CKM software then constructs a key when needed. The client CKM software destroys the key it created, but does not destroy a key that it received from the server, nor does it destroy the authorization token. This is quite different from the present invention, in which client software destroys the key that it receives from the server.

Since the client CKM software only destroys the key it created, it still has all the information (such as the token) to create the key again. In contrast, in the present invention, once the decrypt key retrieved from the server is destroyed, the client does not have the necessary information and hence cannot recreate the key. Accordingly, even if the teachings of Peterka et al. were to be modified by the teachings of Stirling, i.e. CKM software was included, a client would still have all necessary information to decrypt encrypted content by simply recreating decryption keys, which is completely contrary to the present invention.

Applicant submits that the Examiner has applied hindsight analysis in rejecting claim 2. Both Peterka et al. and Stirling et al. fail to teach or fairly suggest encrypting a plurality of sections of data content with a corresponding plurality of encryption keys and distributing decryption keys corresponding to the encryption keys to the processing platform of a consumer in a manner such that the consumer processing platform has simultaneous possession of at most a subset of the plurality of decryption keys, as recited in independent claim 1. Dependent claim 2 depends on independent claim 1 and recites in part that a first decryption key is destroyed after a second decryption key is received, which means that the consumer processing platform has simultaneous possession of at most a subset, in this case two, of the plurality of decryption keys. Applicant submits that the Examiner is incorrect in equating the destroying of a decryption key when it is no longer needed by the decryption engine, as taught by Stirling et al., with the destroying of a first decryption key at a customer processing platform after receiving a second decryption key, as recited in claim 2. There is no suggestion in Peterka et al. that any of the decryption content keys (CK) or program segment keys (PSK) are destroyed, let alone that any key is destroyed after a subsequent key is received. The suggestion in Stirling et al. that a decryption key is destroyed after a decryption engine is finished with it, is not sufficient to allow one skilled in the art to arrive at the subject matter of claim 2, namely that a first decryption key is destroyed after a second decryption key is received.

With regard to the Examiner's rejection of claims 3 to 6, the Examiner has relied upon the same paragraph in Stirling et al., namely paragraph [0080], in rejecting claims 3 to 6 as was relied upon in the rejection of claim 2. Each of the arguments presented in response to the Examiner's rejection of claim 2 are equally applicable to the Examiner's rejection of claims 3 to 6. Applicant submits that claims 3 to 6 distinguish over the teachings of Peterka et al. and Stirling et al. alone and in combination for at least the same reasons as claim 2.

With regard to the Examiner's rejection of claims 16 and 21, the Examiner has relied upon the same portion of Stirling et al., namely paragraph [0080], in support of the rejection of claims 16 and 21 as was relied upon in the rejection of claims 2 to 6. Applicant submits that the arguments presented above with regard to the rejection of claim 2 are also applicable to the rejection of claims 16 and 21. Furthermore, paragraph [0080] of Stirling et al. merely recites that a decryption key may be created when necessary and **destroyed when no longer needed by the decryption engine**. This recitation by Stirling et al. does not recite "destroying the decryption key **after completing playback of the encrypted section**" (emphasis added), as recited in claims 16 and 21. As described above, Peterka et al. is entirely silent with regard to the destroying of encryption keys after decryption and therefore a combination of Peterka et al. and Stirling et al. would not allow one skilled in the art to arrive at the present invention.

Applicant submits that a *prima facie* case of obviousness cannot be made against claims 16 and 21, as the cited references fail to teach all of the claimed limitations of claims 16 and 21.

With regard to the rejection of claim 17, the Examiner has once again relied on paragraph [0080] of Stirling et al. in the rejection of claim 17. As described above, paragraph [0080] of Stirling et al. relates to the creation of **a decryption key** when necessary and the destroying of **the decryption key** when no longer needed by the decryption engine. Applicant submits that paragraph [0080] of Stirling et al., and Stirling et al. as a whole, does not teach or fairly suggest "destroying **decrypted data content** at the customer processing platform **after completing playback of the encrypted section**" (emphasis added), as recited in claim 17. It is respectfully requested that the Examiner identify a specific portion of Stirling et al. that discloses "destroying **decrypted data content**", as it is respectfully submitted that Stirling et al. merely discloses destroying a constructed **decryption key**.

Applicant submits that a *prima facie* case of obviousness cannot be made against claim 17, as the cited references fail to teach all of the claimed limitations of claim 17.

With regard to the rejection of claims 18 and 19, Applicant submits that claims 18 and 19 depend on claim 16 and therefore distinguish over the teachings of Peterka et al. and

Stirling et al., alone or in combination, for at least the same reasons as claim 16, as provided above.

With regard to the rejection of claim 22, similar to the rejection of claims 10, 11 and 12, the Examiner has mistakenly relied upon the recitation in Peterka et al. that a encryption key, i.e. a content key (CK), may be encrypted with a key higher in the key hierarchy, i.e. a unique key (UK), for the purposes of multicast transmission, in rejecting claim 22. Claim 22 recites that "each encryption key comprises a respective customer processing platform-specific key which is determined based on an IP address of the customer processing platform". Applicant submits that encrypting a content key for the purposes of multicast transmission is completely different than encrypting the plurality of sections of data content with a plurality of customer processing platform-specific keys which are determined based on an IP address of the customer processing platform.

According to the teachings of Peterka et al., the encrypted content keys are decrypted with the higher level key, i.e. the unique key (UK), and the content keys are then used to decrypt the corresponding program segments. Once the content key is decrypted with the higher level key, it is completely untraceable, as any customer specific information has been stripped during the decryption of the content key. In contrast, the method according to claim 22 provides for traceability of the decryption key and the encrypted data content, because the sections of data content are encrypted with customer processing platform-specific keys.

Applicant submits that a *prima facie* case of obviousness cannot be made against claim 22, as the cited references fail to teach all of the claimed limitations of claim 22.

With regard to the rejection of claim 23, Applicant submits that claim 23 depends on claim 16 and therefore distinguish over the teachings of Peterka et al. and Stirling et al., alone or in combination, for at least the same reasons as claim 16, as provided above.

With regard to the rejection of claim 39, similar to the Examiner's rejection of claims 16 and 21, Applicant submits that the arguments presented above with regard to the rejection of claim 2 are also applicable to the rejection of claim 39. Furthermore, the Examiner has once again relied on paragraph [0080] of Stirling et al., which as described above merely recites that a decryption key may be created when necessary and **destroyed when no longer needed by the decryption engine**. This recitation by Stirling et al. does not recite "means for destroying the decryption key, **after completing playback of the encrypted section**" (emphasis added), as recited in claim 39. As described above, Peterka et al. is entirely silent with regard to the destroying of encryption keys after decryption and therefore a combination of Peterka et al. and Stirling et al. would not allow one skilled in the art to arrive at the present invention.

Applicant submits that a *prima facie* case of obviousness cannot be made against claim 39, as the cited references fail to teach all of the claimed limitations of claim 39.

In view of the foregoing, Applicant respectfully submits that a *prima facie* case of obviousness cannot be established against claims 2-6, 16-19, 21-23 and 39, since one or more key limitations of each of the claims is missing from both of the cited references. Applicant respectfully submits that claims 2-13, 16-19, 21-23, and 39 are patentable over Peterka et al. and Stirling et al. since a case of *prima facie* obviousness cannot be established.

3. Whether claim 14 is unpatentable under 35 U.S.C. 103(a) over Peterka et al. in view of Ginter et al. (U.S. Patent Application Publication No. 2006/0218651).

In Paragraph 5 on page 23 of the Final Office Action dated March 29, 2007, the Examiner has rejected claim 14 under 35 U.S.C. § 103(a) as being unpatentable over Peterka et al. in view of Ginter et al. (U.S. Patent Application Publication No. 2006/0218651 A1).

To begin, Applicant respectfully submits that a first criterion required to establish a case of *prima facie* obviousness has not been satisfied. That is, the prior art references do not teach all of the claimed features.

With regard to the rejection of claim 14, Applicant submits that claim 14 depends on claim 1 and therefore distinguishes over the teachings of Peterka et al. for at least the same reasons as claim 1, namely that Peterka et al. fails to teach or fairly suggest that decryption keys are delivered "in a manner such that the customer processing platform has simultaneous possession of at most a subset of the plurality of decryption at any time".

Applicant submits that a *prima facie* case of obviousness cannot be made against claim 14, as the cited references fail to teach all of the claimed limitations of claim 14.

4. whether claim 20 is unpatentable under 35 U.S.C. 103(a) over Peterka et al. in view of Stirling et al. and further in view of Ginter et al.

In paragraph 5 on page 24 of the Final Office Action dated March 29, 2007, the Examiner has rejected claims 20 and 43 under 35 U.S.C. § 103(a) as being unpatentable over Peterka et al. in view of Stirling et al. and further in view of Ginter et al.

To begin, Applicant respectfully submits that a first criterion required to establish a case of *prima facie* obviousness has not been satisfied. That is, the prior art references do not teach all of the claimed features.

Claim 20 depends on claims 16. In view of the arguments presented above regarding the Examiner's rejection of claim 16, Applicant submits that Peterka et al. and Stirling et al. fail to teach or fairly suggest key limitations of claim 16 and hence of claim 20. Applicant submits that Ginter et al. similarly fails to teach or fairly suggest these key limitations and therefore claim 20 distinguishes over the teachings of Peterka et al., Stirling et al. and Ginter et al. both alone and in combination.

5. whether claim 34 is unpatentable under 35 U.S.C. 103(a) over Peterka et al. in view of Negawa (U.S. Patent Application Publication No. 2003/0046539).

In paragraph 6 on page 25 of the Final Office Action, the Examiner has rejected claim 34 under 35 U.S.C. § 103(a) as being unpatentable over Peterka et al. in view of Negawa (U.S. Patent Application Publication No. 2003/0046539 A1).

To begin, Applicant respectfully submits that a first criterion required to establish a case of *prima facie* obviousness has not been satisfied. That is, the prior art references do not teach all of the claimed features.

The Examiner has pointed to paragraph [0078] of Negawa in support of the rejection of claim 34, alleging that this paragraph teaches "a method of causing a key for a preceding portion of the encrypted data to be deleted from the customer data content processing device", as recited in claim 34. Applicant submits that Negawa recites "a multicast communication system having a multicast server and a plurality of clients belonging to a multicast group. The multicast server **transmits data encrypted by using a first encryption key** to the clients by multicasting, and **transmits the results of encrypting the first encryption key by using a second encryption key** by unicasting to a client subscribed to a data distribution service, among the plurality of clients. The client subscribed to the data distribution service receives the encrypted data and the result. **The client decrypts the result to obtain the first encryption key and decrypts the encrypted data using the first encryption key**" (see Abstract; emphasis added).

According to the teachings of Negawa, a client device plugs into a distribution data receiving device (see Figure 4) in order to receive encrypted data content and decryption keys from a content server (see Figure 2). The distribution data receiving device includes a key decryption key holding unit 34 that holds a key decryption key Km. Key decryption key Km is the "second encryption key" that is used to encrypt the "first encryption key", which is called the group decryption key Kgr. "Key decryption key Km is preferably stored (formed) in key decryption key holding unit 34 in the form of a hardware circuit (for example an IC chip) to ensure that key decryption key Km cannot easily be read by a third party" (see [0058]).

Paragraph [0078] of Negawa recites that "[w]hen control unit 30 **receives a withdrawal request** from client 3c, it deletes (or destroys) the key decryption key Km(C) held in key decryption key holding unit 34 and deletes (or destroys) the group session key Kgr held in key decryption unit 33". In other words, when the client 3c no longer wishes to decrypt further data content, i.e. the client 3c issues a withdrawal request, the control unit 30 destroys or deletes the key decryption key Km(C) and the group session key Kgr.

This is completely different than "for each subsequent portion of the encrypted data: transmitting to the customer data content processing device a different key to decrypt the subsequent portion of the encrypted data; and causing a key for a preceding portion of the encrypted data to be deleted from the customer data content processing device", as recited in claim 34. For example, according to Negawa, the key decryption key Km is needed to decrypt the unicast message containing the session key Kgr.

If the key decryption key Km is deleted or destroyed then there would be no point in "transmitting to the customer data content processing device a different key to decrypt the subsequent portion of the encrypted data" as the customer data content processing device would be unable to decrypt the "different key" in order to decrypt the "subsequent portion of the encrypted data".

It should be noted that Negawa teaches that a higher level decryption key, namely the key decryption key Km, is destroyed or deleted, thus preventing the decryption of a further lower level decryption key such as the session key Kgr. Accordingly, not only does Negawa fail to teach or fairly suggest the particular feature that the Examiner alleges, but modifying the method of Peterka et al. by incorporating the method of higher level key deletion according to Negawa would render Peterka et al. unsuitable for its intended purpose. Peterka et al. teaches a hierarchy of encryption keys for multicast distribution of encrypted digital content.

According to Peterka et al. a content key (CK) is used to encrypt a section of digital content and the content key (CK) is then encrypted with one or more keys that are higher in the key hierarchy than the encryption key. For example, the content key (CK) may be encrypted with a program segment key (PSK) that is in turn encrypted with a unique key (UK) that is unique to a consumer and allows the consumer to decrypt the PSK and hence the CK.

If the unique key (UK) of the consumer's processing platform is deleted, the consumer would be only unable to decrypt the PSK and hence the CK for subsequent content segments, but would also cause the consumer to be unable to request subsequent PSKs, due to the fact that the UK is required to "initiate the key request message exchange with a particular caching server" (see [0097] of Peterka et al.). If the UK is deleted, the customer would have to re-register with the content provider in order to receive a new UK, which would render the teachings of Peterka et al. unsuitable for its intended purpose.

Applicant submits that a *prima facie* case of obviousness cannot be made against claim 34, as the cited references fail to teach all of the claimed limitations of claim 34 and the incorporation of the subject matter of Negawa would render the operation of Peterka et al. unsuitable for its intended purpose.

Conclusions

With respect to each of the issues presented herein for review, Applicant respectfully submits that errors have been made in the rejection of the appealed claims.

Regarding the issue of whether claims 1, 7-13, 15 and 35-38 are unpatentable under 35 U.S.C. 102(e) as being anticipated by Peterka et al. (U.S. Patent Application Publication No. 2002/0170053), Applicant respectfully requests that the rejection of claims 1, 7-13, 15 and 35-38 be reconsidered by the Board and withdrawn.

Regarding the issue of whether claims 2-6, 16-19, 21-23 and 39 are unpatentable under 35 U.S.C. 103(a) over Peterka et al. in view of Stirling et al. (U.S. Patent Application Publication No. 2003/0223583), Applicant respectfully requests that the rejection of these claims be reconsidered by the Board and withdrawn.

Regarding the issue of whether claim 14 is unpatentable under 35 U.S.C. 103(a) over Peterka et al. in view of Ginter et al. (U.S. Patent Application Publication No. 2006/0218651), Applicant respectfully requests that the rejection of this claim be reconsidered by the Board and withdrawn.

Regarding the issue of whether claim 20 is unpatentable under 35 U.S.C. 103(a) over Peterka et al. in view of Stirling et al. and further in view of Ginter et al., Applicant respectfully requests that the rejection of claim 20 be reconsidered by the Board and withdrawn.

Regarding the issue of whether claim 34 is unpatentable under 35 U.S.C. 103(a) over Peterka et al. in view of Negawa (U.S. Patent Application Publication No. 2003/0046539), Applicant respectfully requests that the rejection of this claims be reconsidered by the Board and withdrawn.

Respectfully submitted,

VINCENT SO

By ______________

Allan Brett
Reg. No. 40,476
Tel.: (613) 232-2486 ext. 323

Date: September 19, 2007

RAB:JFS:sng

Claims Appendix

1. (Original) A method of delivering data content from a data content provider to a customer processing platform and controlling use of the data content at the customer processing platform, comprising:

encrypting each of a plurality of sections of the data content using a respective one of a plurality of encryption keys to produce a corresponding plurality of encrypted sections;

delivering the plurality of encrypted sections to the customer processing platform; and

delivering to the customer processing platform a plurality of decryption keys corresponding to the plurality of encryption keys, wherein the decryption keys are delivered in a manner such that the customer processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time.

2. (Original) The method of claim 1, wherein delivering to the customer processing platform a plurality of decryption keys comprises:

delivering to the customer processing platform a first key of the plurality of decryption keys for a first encrypted section of the plurality of encrypted sections;

delivering to the customer processing platform a second key of the plurality of decryption keys for a second encrypted section of the plurality of encrypted sections; and

causing the first key to be destroyed at the customer processing platform.

3. (Original) The method of claim 1, wherein delivering to the customer processing platform a plurality of decryption keys comprises:

delivering to the customer processing platform a current key of the plurality of decryption keys for a current encrypted section of the plurality of encrypted sections to be processed at the customer processing platform;

delivering to the customer processing platform a next key of the plurality of decryption keys for a next encrypted section of the plurality of encrypted sections to be subsequently processed at the customer processing platform upon completion of processing of the current encrypted section; and

causing the current key to be destroyed at the customer processing platform.

4. (Original) The method of claim 3, wherein delivering to the customer processing platform a next key of the plurality of decryption keys and causing the current key to be destroyed at the customer processing platform are repeated for each of the plurality of encrypted sections to be subsequently processed.

5. (Original) The method of claim 3, wherein the current encrypted section is a first one of the plurality of encrypted sections, and wherein delivering to the customer processing platform a next key of the plurality of decryption keys and causing the current key to be destroyed at the customer processing platform are repeated for each of the plurality of encrypted sections following the first encrypted section.

6. (Original) The method of claim 1, wherein delivering to the customer processing platform a plurality of decryption keys comprises:

providing key control software to the customer processing platform, the key control software being adapted to:

receive a decryption key for one of the plurality of encrypted sections;

complete decryption of the one section; and

destroy the decryption key.

7. (Original) The method of claim 1 further comprising:

billing a customer for delivery of the encrypted sections, and then billing the customer each time the data content is used at the customer processing platform.

8. (Original) The method of claim 1, wherein the data content is video content or music content, and wherein use of the data content at the customer processing platform comprises decryption and playback of the data content.

9. (Original) The method of claim 1, wherein each of the plurality of encryption keys comprises a respective symmetric cryptographic key, and wherein each of the plurality of decryption keys comprises the symmetric cryptographic key of its corresponding encryption key.

10. (Original) The method of claim 1, further comprising:

generating each of the plurality of encryption keys using an identifier associated with the customer processing platform, to thereby generate a plurality of customer processing platform-specific keys.

11. (Original) The method of claim 10, wherein generating comprises generating each of the plurality of customer processing platform-specific keys using the identifier and a respective key generation seed value.

12. (Original) The method of claim 11, wherein delivering to the customer processing platform a plurality of decryption keys comprises delivering the respective key generation seed values.

13. (Original) The method of claim 1, further comprising:

generating a respective transmission value for each of the plurality of encryption keys using an identifier associated with the customer processing platform,

wherein delivering to the customer processing platform a plurality of decryption keys comprises delivering the transmission values.

14. (Original) The method of claim 1, further comprising:

delivering the plurality of encrypted sections from the customer processing platform to a second customer processing platform; and

delivering the plurality of decryption keys from the data content provider to the second customer processing platform, wherein the decryption keys are delivered in a manner such that the second customer processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time.

15. (Original) A computer-readable medium storing instructions which, when executed by a processor at a data content provider, perform a method according to claim 1.

16. (Original) A method of receiving and controlling playback of data content at a customer processing platform, comprising:

receiving over a communications medium a plurality of encrypted sections of data content, each of which has been encrypted using a respective encryption key; and

for each encrypted section:

receiving a decryption key in respect of the encrypted section;

decrypting and playing back the encrypted section using the decryption key; and

destroying the decryption key after completing playback of the encrypted section.

17. (Original) The method of claim 16, further comprising, for each encrypted section:

destroying decrypted data content at the customer processing platform after completing playback of the encrypted section.

18. (Original) The method of claim 16, wherein the communications medium is the public Internet.

19. (Original) The method of claim 16, wherein, for each encrypted section, the encryption key is the same as the decryption key.

20. (Original) The method of claim 16, wherein receiving the plurality of encrypted sections of the data content comprises receiving the plurality of encrypted sections of the data content from another customer processing platform.

21. (Original) A computer-readable medium storing instructions which, when executed by a customer processing platform, perform a method according to claim 16.

22. (Original) The method of claim 16, wherein each encryption key comprises a respective customer processing platform-specific key which is determined based on an IP address of the customer processing platform.

23. (Original) The method of claim 16, wherein receiving each decryption key comprises receiving a transmission value that is determined based on the decryption key and a hardware identifier associated with the customer processing platform, further comprising, for each encrypted section:

recovering the decryption key from the transmission value.

24.–33.(Cancelled)

34. (Original) A method for controlling use of encrypted data content downloaded to a customer data content processing device, comprising:

receiving a request comprising customer verification information from a customer data content processing device;

comparing the customer verification information with corresponding stored customer information ; and

where the customer verification information is consistent with the stored customer verification information:

billing a usage charge to an account of the customer;

transmitting to the customer data content processing device a digital key to decrypt a current portion of the encrypted data content; and

for each subsequent portion of the encrypted data:

transmitting to the customer data content processing device a different key to decrypt the subsequent portion of the encrypted data; and

causing a key for a preceding portion of the encrypted data to be deleted from the customer data content processing device.

35. (Previously Presented) A computer readable medium storing software code executable by a processing platform, the software code comprising:

first software code for coordinating downloading a plurality of sections of data content each encrypted with a respective one of a plurality of encryption keys to a customer computer system from a data content service provider system or another customer computer system; and

second software code for establishing a connection with the data content service provider system to obtain permission to use the data content, and for using the data content where permission is obtained from the data content service provider system by receiving a corresponding one of a plurality of decryption keys for each encrypted section of data content and decrypting the encrypted section using the corresponding one of the plurality of decryption keys such that the processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time.

36. (Original) The computer readable medium of claim 35, wherein the second software code obtains further permissions from the data content service provider system to continue using the data content.

37. (Previously Presented) A signal embodied on a transmission medium containing software code executable by a processing platform, the software code comprising:

first software code for coordinating downloading a plurality of sections of data content each encrypted with a respective one of a plurality of encryption keys to a customer computer system from a data content service provider system or another customer computer system; and

second software code for establishing a connection with the data content service provider system to obtain permission to use the data content, and for using the data content where permission is obtained from the data content service provider system by receiving a corresponding one of a plurality of decryption keys for each encrypted section of data content and decrypting the encrypted section using the corresponding one of the plurality of decryption keys such that the processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time.

38. (Original) A system for delivering data content from a data content provider to a customer processing platform and controlling use of the data content at the customer processing platform, comprising:

means for encrypting each of a plurality of sections of the data content using a respective one of a plurality of encryption keys to produce a corresponding plurality of encrypted sections;

means for delivering the plurality of encrypted sections to the customer processing platform; and

means for delivering to the customer processing platform a plurality of decryption keys corresponding to the plurality of encryption keys, wherein the decryption keys are delivered in a manner such that the customer processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time.

39. (Original) The system of claim 38, wherein the customer processing platform comprises:

means for requesting the data content to be delivered to the customer processing platform;

means for receiving the plurality of encrypted sections;

means for receiving, for each encrypted section, the decryption key in respect of the encrypted section;

means for decrypting and playing back the encrypted section using the decryption key; and

means for destroying the decryption key, after completing playback of the encrypted section.

40. (Original) A data content distribution system comprising:

a data content server configured to receive download requests and permission requests for data content, to encrypt a plurality of sections of requested data content using respective encryption keys to thereby generate a plurality of encrypted sections and to transmit the encrypted sections of the data content in response to a received download request for the data content, and to transmit each of a plurality of decryption keys respectively corresponding to the encryption keys in response to a permission request for the data content; and

a data content download controller configured to generate download requests, to receive encrypted sections of data content in response to download requests, to generate permission requests when downloaded data content is to be used, and for each encrypted section of data content to be used, to receive a corresponding one of the plurality of decryption keys, and to decrypt the encrypted section using the corresponding one of the plurality of decryption keys.

41. (Original) The system of claim 40, comprising a data network connecting the data content server and the data content download controller.

42. (Original) The system of claim 41, further comprising a plurality of data content download controllers connected to the data network.

43. (Original) The system of claim 42, wherein each of the plurality of data content download controllers is implemented in conjunction with a respective customer computer system and is further configured to download encrypted sections of data content from other customer computer systems.

Evidence Appendix

None

Related Proceedings Appendix

None